⑲日本国特許庁(JP)　　⑪特許出願公開

⑫公開特許公報(A)　　昭54—124653

⑤1Int. Cl.²	識別記号	⑤2日本分類	庁内整理番号	⑬公開　昭和54年(1979)9月27日
G 06 F 15/30		97(7) J 1	7165—5B	発明の数　1
G 07 F 7/10		115 D 0	6784—3E	審査請求　有
G 07 G 5/00			6784—3E	(全19頁)

⑤4取引端末装置

⑳特　願　昭54—22064
㉒出　願　昭54(1979)2月28日
優先権主張　㉜1978年3月1日㉝米国(US)
㉛882529

⑦2発明者　ロバート・ウイツトコーム・アンダーソン
アメリカ合衆国カリフオルニア州サン・ホセ・デザート・フレーム・ドライブ6301番地
同　ステイーブン・フランクリン・ブロツク
アメリカ合衆国カリフオルニア州サン・ホセ・アンテイカ・ドライブ5857番地
⑦2発明者　メイ・リユウ・ギイ
アメリカ合衆国カリフオルニア州サン・ホセ・コリブリ・コート216番地
⑦1出願人　インターナシヨナル・ビジネス・マシーンズ・コーポレーシヨン
アメリカ合衆国10504ニユーヨーク州アーモンク(番地なし)
⑦4復代理人　弁理士　頓宮孝一

明　細　書

1.発明の名称　取引端末装置

2.特許請求の範囲

ホストに接続することが出来、取引を承任する為の取引端末装置において、

各々が暗号キーを含む、発行者に独特の複数個の制御ブロックを貯蔵する貯蔵手段と、

使人が端末装置に呈示した識別カード上の、発行者識別データ及びカード検証データを含む符号化データを読取るカード読取手段と、

前記発行者識別データに応答して対応する制御ブロックがあるかどうか前記貯蔵手段を探索する手段と、

前記貯蔵手段の中に対応する制御ブロックが見つからない時に前記符号化データを前記ホストに連絡すると共に、前記貯蔵手段に書込む為に前記ホストから対応する制御ブロックを受取る手段と、

前記対応する制御ブロックからの暗号キー・データに応答して前記カード検証データを暗号化してカード検査番号を発生する手段と

を有する取引端末装置。

3.発明の詳細な説明

この発明は取引実行装置、更に具体的に言えば、遠隔端末装置と連絡する中央データ・ベースを持つていて、複数個の協働する機関の内の任意の1つによつて発行された機械が読取り得る識別カードに応答して、現金の支払又は資金の口座間の振込みの様な取引の実行が出来る様にする取引実行装置に関する。

公共の便宜並びに経済性の為、利用者から要請された取引を実行する種々のシステムが開発されている。その一例は小切手現金化機である。この機械は挿入された小切手からデータを読取り、小切手が正しいと認められた場合、小切手の額に相当する現金を支払う。クレジット・カードを使う他のシステムも開発されている。

1つのクレジット・カード・システムは、中央データ・ベースにクレジット・カード口座情報を貯蔵している。遠隔端末装置から口座番号が提示さ

れたことに応答して、システムが口座に関する情報を供給する。例えば、システムは、カードが切れていること、盗まれていること、又は残高を表示することが出来る。取引が完了した後、システムは貯蔵情報を正しく調節して、この取引の帳じりを合せる。

業務が混む時間又は時間外にその営業を拡張する為に屢々銀行によつて使われているクレジット・カード・システムの他の例では、端末装置を介して現金を支払い又は預金を受領することが出来る様にしている。典型的には、このような端末装置はクレジット・カードを受入れて、それから情報を読取る機構、キーボード、表示装置及び紙葉出入れ孔を含んでいる。端末装置はデータベースと共に動作することも出来るし、或いは単独の装置として動作することも出来る。各々のクレジット・カードに個人ＩＤ（識別）番号を与えることにより、人間が介在しなくても、現金の支払の際の安全性を高めることが出来る。この時、クレジット・カードによる取引は、クレジット・カー

（3）

発行したクレジット・カードを所定の端末装置で使える様にする場合、これら全ての銀行は同じ符号又はアルゴリズムを使うか、或いは口座データからＩＤ番号を導き出すのに使われるアルゴリズム関係を他の何等かの形で識別出来る様にしなければならない。この様な１つのシステムでは、各々の端末装置に同一の疑似乱数表を用意する。乱数表は、最初は機関の識別子で、次に表の出力と口座番号の数字との論理的な組合せによつて準不規則的にアドレスされる。このシステムでは、種々の銀行が発行したカードを使うことが出来るが、各々の銀行の人間は、その端末装置で他の全ての銀行が使うアルゴリズムに対する手がかりを持ち、銀行識別子符号が判つていれば、ＩＤ番号を容易に再生することが出来る。別のシステムでは、キーによつて作用するアルゴリズムを用意して、ＩＤ番号と口座番号との間の関係を決定する。このシステムでは、線形及び非線形操作を使つて、口座番号とキー番号とを組合せ、ＩＤ番号と比較される検査番号を発生する。米国特許第３９５６６

（5）

ドから読取つた口座番号に対応するＩＤ番号がキーボードから送込まれた時にだけ出来るようになる。この所要の対応性により、泥棒や単にクレジット・カードをみつけた者が、端末装置から現金を受取ることが出来ない様にする。端末装置がデータベースと一緒に作用する時、口座番号とＩＤ番号との間の対応性は無作為に選ぶことが出来るが、ＩＤ番号は予定の符号に従つて口座番号から導き出せる様にする場合が多い。この場合、ＩＤ番号を顧客による選択等によつて無作為に選べる様にする為に、カードには口座番号と共にずらし（オフセット）数値が記録される。このずらし数値は、予定の符号に従つて口座番号から導き出された番号に加えるか又はその他の形でそれと組合せた時、その結果が無作為に選んだＩＤ番号になる様に選ばれる。ＩＤ番号とカードの口座（並びにずらし）データとの間のこの予定の関係により、単独の端末装置が、ＩＤ番号をアルゴリズムによつて口座番号に関係づけることにより、ＩＤ番号を検査することが出来る。複数個の協働する銀行が

（4）

１５号にこのシステムが記載されている。然し、異なる銀行が発行したカードを同じ端末装置で使える様にする為には、全ての銀行が同じキー番号を使わなければならないし、口座番号は全てのカードで同じフイールドになければならない。この米国特許のシステムを改良した１つの形式では、暗号キー表を各々の端末装置に用意しておき、表には、キーボードから送込んだＩＤ符号と比較する為の検査番号を発生する為に使われる口座、ずらし並びにその他のデータのカードのデータ・トラック上での位置を特定するデータと共に、複数個の協働する銀行に対して、キー作用形アルゴリズムに使うのに必要なキーを入れておく。然し、このシステムはこの様な表の規模に対する貯蔵装置の制約を受け、各々の端末装置は、少数の選ばれた協働機関が発行したカードでしか動作することが出来ない。更に、このシステムは、銀行がその発行カードの基準を２つの異なる形式の間で変えている時に起る様に、機関のＩＤ及びカード状態が同一であつて形式が異なるカードに対処する

（6）

ことが出来ない。

表から導き出したキーによつて作用するクレジット・カード及びＩＤ番号確認方式は、各々の現金支払端末装置の安全性を改善すると共に他の銀行が発行したカードを引受ける点で、複数個の銀行が協働出来る様にするが、端末装置に貯えられているか、或いは協働する銀行の口座にあつて、端末装置の動作によつて資金どうしの間の振込みが可能な大金の奪取をねらわれる弱点がある。重大な１つの問題は、単独動作が出来るか或いはオンライン動作も出来る端末装置の暗号アルゴリズムの安全性である。今日、現金支払端末装置の業務を行なう為には、非常に多数のオペレータ又は保守人員が必要である。例えば銀行の各支店の１人又は２人は、現金支払端末装置に内部接近することが出来る。こういう人員は、通常の保守の為に暗号キーにも接近出来る場合が多い。或いはその代りに、僅かな訓練しか受けていなくても、こういう人員は、内部回路の電気信号を測定することによつて、キーを入手する方法を覚える惧れが

データベースの口座内にある資金をだまして振込む惧れがある。

この発明の取引実行装置は、多くの口座に対する貯蔵情報のデータベースを持つホスト・データ処理装置と、複数個の取引端末装置とを含む。各々の端末では、複数個のカード発行者に対して暗号キー及びカード形式情報の表を保持しておき、取引を行なう許可を求める個人が端末装置に提示した識別カードから読取つた発行者のＩＤに応答して、この端末装置の表を探索する。発行者のＩＤが端末装置の表に見つからない場合、端末装置がカード・データをホストに連絡すると、ホストがマスター表を同様に探索する。発行者に対するマスター表の項目は、取引に使う為に、ホストから端末装置に連絡され、その後端末装置の表から追放することができる。ホストは消費者の情報のファイルを検査して、この情報の示す通り、カードを保存すること、取引を停止すること、又はその他の処置を端末装置に命令することが出来る。更に、局地のホストが別の遠隔のホストと連絡し

ある。一旦暗号キーが入手されれば、アルゴリズムが判ると、非常に多数の口座番号とＩＤ番号との間の対応性を作り出すことが出来る。その場合、カードの形式とカード上の検証データ及びずらしデータの場所とが判つていれば、カードのデータと無作為に選んだＩＤ番号との間の対応性を確かめることが出来る。

端末装置とホストのデータベースとの間で口座情報及びＩＤ情報を伝送することによつても、別の保安上の問題が起り得る。こういう伝送には、公共通信線路が使われる場合が多く、その為非常に多数の人間から監視される惧れがある。通信の安全性を改善する為に暗号が使われる場合が多いが、この符号を見破ることが出来た者、又は符号を入手することが出来た者は、この伝送を監視することにより、クレジット・カードの口座情報とＩＤ番号との間の対応性を導き出して、そのリストを編集することが出来るようになろう。更に、偽の端末通信トラヒックを発生することにより、或る者がホストのデータベースに連絡をつけて、

て、端末装置からの取引の要請を予想して、局地のホストのデータベースに消費者の情報を入れておくことができる。

暗号キーはホスト及び端末装置の両方の表に暗号形式で貯蔵され、通信の時は２重に暗号化される。

暗号キー及びカード形式の表は、端末装置のカード読取機によつて決定されたカード・トラック状態に応答して、接近出来るようにする。

第１図について説明すると、この発明は、複数個の銀行又はその他のカード発行機関によつて発行された個人識別カードを使つて、複数個の個人が自動銀行端末機等を作動することを許可する装置を提供する。各々の端末装置は、識別カードから読取つたデータと、個人がキーボードから送込んだデータとの間の対応性を検証する為に使う暗号キーを含む金融機関表（ＦＩＴ）を備えている。端末装置のＦＩＴに項目を持つていない機関によつて発行されたカードが端末装置に提示された時、端末装置がホストＣＰＵにあるマスターＦＩＴに

連絡することが出来るようにすることにより、ＦＩＴは事実上規模が無制限である。

端末装置１は例えば交換システムにおける地理的に分散した複数個の自動銀行端末機（ＡＴＭ）の内の１つである。こういうシステムでは、複数個の銀行が、他の銀行によつて発行されたＡＴＭカードを自分のものとして引受けることに合意する。

ＡＴＭ１で銀行取引をしようとする個人が、磁気符号化カードをカード読取機２に挿入し、キーボード３から自分の個人識別番号（ＰＩＮ）を送込む。カードから読取られた口座番号４又はその他の特定の有効認定データが暗号論理回路５によつて数に変換され、この数が比較器６でＰＩＮ７と対応するかどうか検査される。この検査並びに／又はその他の検査を充たすと、個人は所望の取引を進めることが許される。

各々の銀行は、その顧客に識別カード及びＰＩＮを発行する際、異なるＰＩＮキーk_1、k_2……k_mを使う。ＰＩＮキーは、例えば口座番号

から対応するＰＩＮを導き出す際に暗号論理回路によつて使われる多重ビット数である。ＦＩＴ８に一組のこういうＰＩＮキーk_1、k_2……k_n（ｎ個の銀行又は異なる形式に対し）が貯蔵される。ＦＩＴは、後で更に詳しく説明する様に、トラック状態の選定と共にカード読取機２が読取つた銀行識別フイールド９によつて探索され又はその他の形で呼出される、端末貯蔵装置のアドレス空間内の表である。全ての銀行又は形式に対するマスターＦＩＴ１０をホストＣＰＵ１１で管理し、そして端末のＦＩＴ８が、取引を完了する許可を要請する個人のＩＤカードから読取つた銀行ＩＤ９に対応する項目を持つていない時、端末装置１によつてそのマスターＦＩＴが呼出される。ホスト１１は、銀行ＩＤ９が取引会員のそれに対応することを検証し、そのＦＩＴ１０の項目を端末装置１に連絡する。端末装置１は、この情報を現在並びに今後の取引に使う為、位置Ｎに貯蔵することが出来る。ホスト１１は、ＩＢＭ３６００金融システム用のＩＢＭ３６０１通信制御装置又はＩ

ＢＭシステム／３７０の様な汎用計算機、又はホスト及びサブホストの任意の組合せであつてよいが、これは後で更に詳しく説明する。

後で述べるが、ＦＩＴ表８及び１０は一層多くの情報を持つていてよく、こうして独自のＰＩＮキーだけでなく、カードの形式、認可並びに取引パラメータを限定する融通性を各々の銀行Ｍに与えることができる。

第２図について説明すると、この発明の取引端末装置は、米国特許第３９５６６１５号に記載されている装置の改良である。この米国特許の第２図をこの出願の第２図として再掲し、参照し易くした。第２図の詳しい説明については、米国特許第３９５６６１５号を参照されたい。取引端末装置１をどの様な形で実現するかは、この発明を実施するのに重要ではないが、好ましい実施例が第２図に示されている。端末装置１は全体的にモジュール形であつて、情報母線６２によつて端末装置の複数個のサブシステムに結合されたプログラム式マイクロプロセッサ６０を含んでいる。マイ

クロプロセッサ６０がクロック発生器６４からのクロック信号によつて駆動され、電気的に変更し得る即時呼出し式記憶装置（ＲＡＭ）及び読出専用貯蔵装置（ＲＯＳ）の両方の機能を持つデータ貯蔵モジュール６６に作動的に接続される。データ貯蔵装置６６の内の読出専用貯蔵装置部分が、マイクロプロセッサ６０用の種々の動作プログラムを貯蔵する。データ貯蔵モジュール６６の即時呼出し式記憶装置部分が、プログラムの実行、キー並びにＦＩＴ表１０の貯蔵用のスクラッチパッドになる。プロセッサ支援装置６８、機械的な制御装置７０、利用者通信装置７２、現金支払装置７４、オペレータ機能装置７６及び通信装置７８の動作特性については、米国特許第３９５６６１５号を参照されたい。

この発明の取引許可装置では、利用者の取引要請を実行する間、端末装置とホストとの間で６つの通信メッセージが必要になることがある。これらを第３図乃至第５図について説明するが、次の通りである。

ＶＦＩＴ取引要請
ＶＦＩＴ返答
ＶＦＩＴ状態
取引要請
返答
状態

取引要請、返答及び状態メッセージは、米国特許第３９５６６１５号に記載されているものと同様であるが、この発明では変更が加えられている。ＶＦＩＴメッセージは後に挙げた３つと略同じであるが、取引端末装置１がＦＩＴ項目を得る為にホスト１１に連絡しなければならない時に使われる。

この発明の取引実行装置は、ジ・アメリカン・バンカーズ・アソシエイション及び／又はスリフト・インダストリー・アソシエイションの２磁気ストライプ識別カード形式、及びインターナショナル・スタンダーズ・オーガニゼイション（ＩＳＯ）が提案するトラック３磁気カード形式に合う様になつている。ＩＤ番号とクレジット・カード

びＰＩＮ項目バイトが、端末装置によつて検出されたフラグ特殊状態に加えられる。Ｔ－２及びＴ－３は、カード読取機２が読取ることが出来る識別カードの磁気ストライプ上の２つの別々のデータ・トラックを表わす。

取引要請で、Ｔ－２及びＴ－３データのいずれか一方又は両方を伝送することが出来る。どのＴ－３フィールドを伝送するか並びにどの区域にある情報を送るかを記述するデータ・マップ・フィールドは発行者のＰＩＮ表項目にある。取引要請メッセージには下記のデータが含まれる。

メッセージの見出し
Ｌ—— Ｌフィールドを含めて、メッセージの長さを表わす
Ｎ—— 取引順序番号を表わす
Ｃ—— メッセージのクラス／サブクラス（取引要請／通常又はＶＦＩＴ取引）を表わす

情報との対応性を決定する特定の暗号アルゴリズムは、この対応性が暗号キーに依存するものでなければならないことを別にすれば、この発明を実施する上で重要ではない。米国特許第３９５６６１５号に記載されている暗号アルゴリズムはルシファと呼ばれているが、この発明の装置は、Ｆｅｄｅｒａｌ Ｒｅｇｉｓｔｅｒ 第４０巻、第５２号（１９７５年３月１７日、月曜日）所載のＮａｔｉｏｎａｌ Ｂｕｒｅａｎ ｏｆ Ｓｔａｎｄａｒｄｓの" Ｅｎｃｒｙｐｔｉｏｎ Ａｌｇｏｒｉｔｈｎ ｆｏｒ Ｃｏｍｐｕｔｅｒ Ｄａｔａ Ｐｒｏｔｅｃｔｉｏｎ "（以下ＤＥＳと呼ぶ）を使うのに適している。

取引要請メッセージ

この発明では、米国特許第３９５６６１５号に記載されている取引要請メッセージに対して、次の拡張機能が加えられている。このメッセージは、取引の処理の為にホスト／サブホストに送られる普通の取引情報と共に、Ｔ－３及びＴ－２カード・データを伝送する。メッセージ・フラグ・バイト及

可変フィールド（ＶＡＲ）
各々の引出し要請に対するロールオーバ式札計数器の合計。或いは取引順序番号
消費者ＰＩＮ
消費者又は顧客が送込んだＰＩＮ
口座出フィールド
消費者のキーボードからの記入によつて定められた口座出フィールド
口座入フィールド
消費者のキーボードによる記入によつて定められた口座入フィールド
特殊取引番号フィールド
金額フィールド
札混合フィールド
Ｔ－２カード・データ
メッセージ・フラグ
ビット０ Ｔ－２は良好。
１ Ｔ－３は良好。
２ ＰＩＮ再試行カウントの限界に達する。
３ ＰＩＮ再試行の取消し失敗。正しい

ＰＩＮを送込まなかつた場合、このビットをセットして不完全取引要請が送られる。

4　ＩＤカードがカード読取機の輸送部の裏側に止まつている間に、スイッチの不規則性が検出された場合、カードのひつかかりが起つている惧れがあることを表わすスイッチ不規則性。

5　ＰＩＮ未検査フラグ。端末装置がＰＩＮの検証をしない時、何時でもセットされる。

6　ＩＤカードにトラック２及び３の両方が検出されたことを表わす２トラック・カード。

ＰＩＮ再試行

許される限界に達する前に、顧客が正しいＰＩＮを送込もうとした試行の回数を示す。

Ｔ－３データ・マップ

Ｔ－３カード・データ・フイールド中でどの

に、選択した各々のトラック（Ｔ２、Ｔ３）に対して送るべきデータ量を特定する。ホスト／サブホストは、適当なＰＩＮ表の項目を送ることによつて応答することが出来る。ＶＦＩＴ取引要請メッセージは下記のフイールドを含む。

メッセージの見出し
取引順序番号
メッセージ・フラグ
Ｔ－２データ
Ｔ－３データ

メッセージの見出し及びメッセージ・フラグ・フイールドは、取引要請メッセージに対して上に述べた様に特定される。

取引返答メッセージ

取引返答メッセージはホスト／サブホストが、動作、表示及びステートメント・プリンタ・データと共に、カードに書込む為にＴ３データを送ることが出来る様にする。このメッセージは下記のフ

Ｔ－３フイールドが送られているかを示す。これはこの取引のＩＤカードに対してＰＩＮ表の項目中に発見されるＴ－３データ・マップの写しである。

Ｔ－３カード・データ

Ｔ－３カード・データは、それが首尾よく読取られ、且つＰＩＮ表の項目がそれを送るべきことを示す時に、伝送される。トラック情報の全部又は或るフイールドが、ＰＩＮ表項目のＴ－３データ・マップの指示により、伝送されることがある。

ＶＦＩＴ取引要請メッセージ

この特別の取引要請サブクラス（メッセージの見出し、前掲のバイトＣ）は、（初期プログラム挿入、ＩＰＬで端末装置の初期設定の際）仮想ＰＩＮ表項目機関選択権を選んだ場合、端末装置がホスト／サブホストに仮想ＰＩＮ表項目要請をすることが出来る。この選択権は、仮想ＰＩＮ項目の要請を行なうことが出来るかどうかを特定すると共

イールドを有する。

メッセージの見出し

計数器

ロールオーバ式札計数器の合計の値

動作

このバイトは、下記を含めて、端末装置がとるべき動作を特定する。

0　予め定められた利用者メッセージを表示する。

1　表示データ・フイールドにある利用者メッセージを表示する。

2　ステートメントを印刷する。

3　カード取出しの時間切れ。

4　取引を許可する。

5　クレジット・カードを保有する。

6　利用者の確認を要請する。

7　Ｔ－３データを書込む。

数量１

ホッパ＃１から支払うべき札の数。ホッパが

1台の端末装置ではゼロ。

数量2

支払うべき札の数（ホッパが1台の端末装置）又は貨幣ホッパ#2から支払うべき札の数。

表示データ

これがある場合、表示すべきメッセージ・データを含む。このメッセージは予め定められたメッセージの番号又は特別なメッセージの本文のいずれかであつてよい。

ステートメント・データ

これがある場合、取引ステートメントに印刷すべきデータ、即ち予め定められたメッセージ又は実際のメッセージ或いはその両方の番号。

T－3データ長さ

T－3データ・マップ

T－3データ

VFIT取引返答メッセージ

この特別の取引返答メッセージは、端末装置から要請された時、PIN表の項目を伝送するものであるホスト／サブホストがPIN項目を供給することが出来ない場合、VFIT取引返答はゼロのPIN項目フイールドを持つ。他の場合、動作バイトのビット6が1にセットされていなければ、新しい項目を受取るまで供給されたPIN項目を端末装置の記憶装置に保存する。PIN項目は通信キーC又はキーBに暗号化される。このメッセージは下記のフイールドを有する。

メッセージの見出し

計数器

ロールオーバ式札計数器の合計を端末装置に保管しておき、ホストの適用業務プログラムに保管する。

動作

0　予め定められた利用者メッセージを表示する。

1　表示データ・フイールドにある利用者メッセージを表示する。

4　PIN項目をメッセージに入れる。

5　クレジット・カードを保有する。

6　処理の後にPIN項目を追放する。

計数器1

計数器2

表示データ

PIN項目

状態メッセージ／VFIT状態メッセージ

状態メッセージが、取引返答メッセージに応答して、端末装置からホストに伝送され、返答メッセージで受取つたデータの処理結果を示す。この発明の好ましい実施例に関連する種々の状態ビットの定義は、取引の処理の不規則性並びに仮想PIN項目の返答の際の誤りに関する。状態メッセージに含まれる選ばれたフイールドは次の通りである。

メッセージの見出し

取引順序番号

計数器1

データの長さフイールド

計数器2

状態データ

0　T－3書込み失敗

1　スイッチの不規則性

2　仮想PIN表の項目の誤り。このビットは次の場合にセットされる。

(1)　要請された項目が、発行者のIDの比較及びカードの種類に基づいて、送返された項目に合わない時

(2)　送返された項目が長すぎる時

(3)　PIN長さフイールドの値が所定の値より小さい時

(4)　送返された項目の長さがゼロの値である時、又は

(5)　項目が無効なフイールド位置の仕様を持つ時

3　T－3データの誤り

次に第3図について説明すると、端末装置1で取引を行なおうとする個人が、磁気符号化クレジ

ット・カードをカード読取機２に挿入する。カードから読取られたデータがデータ貯蔵装置６６に貯蔵され、局部ＦＩＴ８を探索する為にマイクロプロセッサ６０によつて利用され、有効認定データ１２、ＰＩＮ検査番号１５を作成するのに使うずらしデータ１３及び通信装置７８によつてホスト１１に伝送する為に取引要請メッセージ１６に入れるデータを供給する。個人は、この取引の処理中の適当な時刻に、自分のＰＩＮ７をキーボード３から送込む様に命令され、マイクロプロセッサ６０内の比較器６でＰＩＮ検査番号１５と比較される。

消費者カードがカード読取機２に正しく挿入された後、端末装置１は、取引に関係する情報を見つけることが出来る様に、且つ消費者が送込んだＰＩＮを検証する次の工程を行なうことが出来る様に、カードから読取られたカード発行機関のＩＤに対するＰＩＮ表（ＦＩＴ）項目を探そうとする。マイクロプロセッサ６０と協働してカード読取機２が行なうトラックの処理は、クレジット・

の探索は、カードが処理し得るものである場合、消費者が挿入したカードに対応するＰＩＮ表の項目を探す試みである。ＰＩＮ表探索アルゴリズムは、発行者識別子（ＩＩ）を探索引数、クレジット・カードのトラック状態を修飾子として使う。探索引数は、ＩＳＯ基準案Ｔ３形式に従つて、カード番式ＩＤ、業界ＩＤ、標準発行者ＩＤ及び消費者の主要口座番号を含む２０個までの連続的なデイジットを含むことが出来る。ＦＩＴ項目が第６図に示されており、後で説明するが、これを次の様に探索する。ＰＩＮ表、又はＦＩＴに特定されている項目種類がカードの種類に合わない場合（例えばＴ－２が良好で、Ｔ－３がクレジット・カードで検出されないが、ＰＩＮ表の項目がＴ－３だけ、Ｔ－２又はＴ－３独立又はＴ－２／Ｔ－３の組合せである場合）、ＰＩＮ表の項目を飛越す。カードの種類がＰＩＮ表の項目の種類に合うと、ＰＩＮ表の項目の定義を使つて、ＰＩＮ表の項目中にある発行者ＩＤと比較するカード・データを突止める。それらが合わない場合、次のＰＩ

カードを読取つて、それがトラック状態に基づいて処理し得るものであるかどうかを判定する。消費者がカード読取機２にカードを挿入する時、トラックが読取られ、必要であれば、各々のトラックに対するトラック状態を判定する為に再び読取られる。状態は良好、不良又は検出不能であることがある。少なくとも１つのトラックが良好状態であれば、カードは使用可能と考えられる。

交換システムの各々の独特な発行者が、ＰＩＮの有効認定及びＰＩＮの暗号化に使うＰＩＮキーを供給する。こういうＰＩＮキーは、初期設定（ＩＰＬ）の際、ホスト１１から端末装置１に伝送される独特なＰＩＮ表８の項目として、交換所の会員機関によつて供給される。この代りに、これらの項目は、仮想ＰＩＮ処理の為、ホストのＦＩＴ１０（第４図）に保持してもよい。

局地のＦＩＴ８を探索する際にマイクロプロセッサ６が行なう工程が、第８図に示されている。ＶＰＩＮ処理の要請に応答して、ホスト１１が同じ工程をとることが出来る。ＰＩＮ表８、１０

Ｎ表の項目に対して同じ過程が繰返される。合致すると、探索が終了し、ＰＩＮ表８のその項目の定義を消費者の取引の残りの処理に使う。普通の項目がこのカードの種類に対してみつからず、仮想ＰＩＮ表の項目の選択権が特定されていない場合、探索はＰＩＮ表８の最後の項目で終了する。合うものが見つからないと、クレジット・カードは消費者に返される。

普通の（即ち対応する）項目がＦＩＴ８に見つからず、端末装置１に対して仮想ＰＩＮ表の選択権が特定されている場合、マイクロプロセッサ６０はＶＦＩＴ取引要請メッセージ１７を組立ててホスト１１に伝送する。ホスト１１は、ホストのＦＩＴ１０を探索し、ＦＩＴ表の項目１９を含むＶＦＩＴ返答メッセージ１８を組立て、端末装置１がＦＩＴ８又はデータ貯蔵装置６０の他の或る領域に貯蔵する様にする。この為、ホスト／サブホスト１１にＶＰＩＮ表の項目を要請する前に、前のＶＰＩＮ要請で内部で保管してあつたＶＰＩＮ項目を、現在のＩＤカードと合うか、どうか検

査する。ホストのＤＩＴ１０に項目が見つからない場合、その事実が、ＶＦＩＴ取引返答メッセージ中の動作バイトのビット４によつて表示される。

消費者のクレジット・カードのデータに対応するＰＩＮ表８の項目が見つかつた後、その項目を検査して、端末装置１又はホスト１１のどちらによつてＰＩＮ有効認定を行なうかを判定する。ホスト１１によるＰＩＮ有効認定が特定されている場合、トラック状態が検査されるが、端末装置１ではこれ以上ＰＩＮの処理が行なわれない。トラック状態が不良トラックであることを表わし、ＰＩＮ表の項目が「不良トラックを持つカードを排除せよ」を特定する時、取引は停止し、カードが消費者に返され、適当なメッセージが表示される。カードが不良トラックを持つていないか、或いはＰＩＮ表の項目が「不良トラックを持つカードを処理せよ」を特定する場合、ＰＩＮの処理が進められる。

暗号アルゴリズム２０で、ＰＩＮ表８からの暗号化されたＰＩＮキーがキーＡを使つて復号され、

(31)

ＦＩＴ項目の内の下記のパラメータが、カード・データに対する長さ、変位及び埋合せの仕様と、１０進化表と、ＰＩＮ検査を行なうのに必要な暗号キーとを定める。

ＶＡＬＤＩＳＰは、カード・データの最初のデータ・デイジットからの有効認定データ・フイールドの変位を定める。

ＶＡＬＬＥＮは、有効認定データ・フイールド中に含まれるデイジットの数を定める。

ＶＡＬＰＡＤは、デイジット数が１６個未満である場合、有効認定データの埋合せに使われるデイジットを定める。

ＯＦＦＤＩＳＰは、カード・データの最初のデータ・デイジットからのずらしデータのフイールドの変位を定める。

ＣＨＡＬＥＮは、ずらしデータ・フイールドに含まれるデイジット数、顧客が送込んだＰＩＮで検査するデイジット数、及び顧客が送込んだＰＩＮに許されるデイジットの最小数を特定するパラメータである。

(33)

後で説明する暗号化工程５に使うＰＩＮキーを発生する。ＰＩＮ検査又は有効認定データ１２及びずらしデータ１３は、いずれかのトラックＴ－２又はＴ－３の何処にあつてもよい。端末装置のＰＩＮ有効認定がＰＩＮ表の項目によつて特定されている場合、その位置はＰＩＮ表の項目によつて記述されている。端末装置１によるＰＩＮ処理はマスター・キー（カード・データ、カードに対して選ばれたＦＩＴ項目からのデータ、及び消費者が送込んだキーボード・データ）を含む。マスター・キーがマスター・キー装入指令で、ホスト１１から端末装置１に送られる。マスター・キー装入指令が実行されていない場合、オペレータ／ＣＥパネル７６から送込んだＡキーをマスター・キーとして使う。有効認定データ１２は消費者の口座番号であつてもよいし、或いは金融機関が消費者を同定する為に使いたい任意の数であつてよい。ずらしデータは随意選択であり、消費者が送込むＰＩＮ及び有効認定データを独立に特定することが出来る様に選ぶことが出来る。

(32)

ＤＥＣＴＡＢは、暗号化された有効認定データを１０進数に変換する為に使われる１６個の１０進デイジットの表である。

ＥＰＩＮＫＥＹは、有効認定データを暗号化する為に使う暗号化されたＰＩＮキー（マスター・キーで暗号化される）である。

キーボード３から下記のデータが送込まれる。

ＰＩＮは顧客によつてキーボード３から送込まれた個人識別番号である。

ＰＩＮ長さは、顧客が送込んだＰＩＮにあるデイジットの数である。

次に第３図について説明すると、端末装置１はホストから切離されたＰＩＮ検査を次の様に行なう。

1. ＶＡＬＤＩＳＰを使つて場所を見つけ、ＶＡＬＬＥＮを使つて長さを決定することにより、カードから有効認定データ１２を求める。

2. 有効認定データ・フイールドにあるデイジット数を表わすＶＡＬＬＥＮが１６未満である場合、ＶＡＬＰＡＤによつて特定されたデイジット

(34)

を使つて、埋合せ工程２１で、１６デイジットの右側で有効認定データ１２の埋合せを行ない、埋合せ有効認定データ２２を作る。

3. 下記の２つの方法のどちらかにより、ＰＩＮキーを求める。

ＦＩＴ表の項目中にＥＰＩＮＫＥＹ（又はＦＩＴキー）パラメータが特定されている場合、マスター・キーを使つてＥＰＩＮＫＥＹの値を復号する。

ＦＩＴ表の項目中にＥＰＩＮＫＥＹパラメータが特定されていない場合、マスター・キーをＰＩＮキーとして使う。

4. ＰＩＮキーを使つて、暗号アルゴリズム５によつて埋合せ有効認定データ２２を暗号化し、暗号化有効認定データ２３を作る。

5. ＤＥＣＴＡＢを使つて、暗号化有効認定データ２３を１０進化ルーチン２４で１０進デイジットに変換し、１０進化有効認定データ２５を作る。暗号化有効認定データ２３の各々の１６進デイジットがＤＥＣＴＡＢからの１０進デイジット

に替えられる。選ばれた１０進デイジットは、ＤＥＣＴＡＢ中のその変位（０－１５）が、有効認定データ２３中で取替えられる１６進デイジット（０－Ｆ）の数値に対応するデイジットである。

6. ＯＦＦＤＩＳＰを使つて場所を探すと共に、ＣＨＫＬＥＮを使つて長さを決定することにより、カードからずらしデータ１３を求める。ＯＦＦＤＩＳＰ＝２５５（Ｘ′ＦＦ′）である場合、ずらしデータに全部ゼロのデイジットを使う。

7. ブロック２６で、ずらしデータ１３を１０進化有効認定データ２５と揃えて、ずらしデータ１３の一番左のデイジットが１０進化有効認定データの一番左のデイジットよりＤ個又は更に多くのデイジット位置だけ右へ変位する様にする。この変位のデイジット位置の数は、ＰＩＮ長さからＣＨＫＬＥＮを差し引くことによつて求められる。

8. ずらしデータのデイジット１３をそれと揃つている１０進化有効認定データのデイジット２５と基数１０でデイジット毎に加算する。その結果がＰＩＮ検査番号１５である。

9. ＰＩＮ検査番号１５を比較器６で、顧客が送込んだＰＩＮ７のデイジットと右側からデイジット毎に比較する。比較が成立する為には、ＰＩＮ検査番号１５の全てのデイジットは、顧客が送込んだＰＩＮ７の対応するデイジットと同じでなければならない。顧客が送込んだＰＩＮ長さがＣＨＫＬＥＮより大きければ、顧客が送込んだＰＩＮ７の一番左側の（最初に送込んだ）デイジットは検査されない。こういう余分のデイジットは任意の値であつてよい。比較６が成立する場合、端末装置１は、データを組立て、その一部分をホスト１１に対する取引要請メッセージ１６に暗号化することにより、取引を進める。比較６が成立しない場合、端末装置１は試行設定パラメータによつて定められる様に、顧客に０回又は更に多くの試行を許す。端末装置１はカードを戻し、ホスト１１にメッセージを全く送らないで、取引を停止することが出来る。この代りに、端末装置１はホスト１１に無効ＰＩＮ取引要請メッセージを送り、カードを戻すか又は保有し、場合によつては顧客

に対してメッセージを表示する様に端末装置１に指示する取引返答を待つ。

第４図には、端末装置１からのＶＦＩＴ取引要請１７を処理する場合のホスト／サブホストが示されている。前掲米国特許第３９５６６１５号の第４図に説明されている手順に従つて、ＶＦＩＴ取引要請メッセージ１７を復号する。局部ＦＩＴ表８の探索について前に述べた様に（並びに第８図に示す手順に従つて）、トラック状態及び発行者識別符号を使つて、付属データ処理装置１１がサブホストＦＩＴを探索し、通信キーＢ又はＣを使つて、暗号アルゴリズム２８で暗号化する為に、対応するＦＩＴ項目１９を突止める。暗号アルゴリズム２８は、Federal Register、第４０巻、第５２号（１９７５年３月１７日（月曜日）号）に記載されているData Encryption Standards（ＤＥＳ）of the National Bureau of Standardsに従つて、付属データ処理装置１１又はデイジタル・ハードウエア論理装置によつて実行される適用業務プログラム

として実現することが出来る。

VFIT取引要請メッセージ17中に、IDカードからのトラック・データとして供給される顧客口座識別データを使つて、付属データ処理装置11がその顧客データ・ファイル29を探索することが出来、そこに貯蔵されている情報に基づいて、VFIT返答メッセージ18中の動作ビットを通じて、カードを保有するか又は取引を停止するか又は取引を承認する様に、端末装置1に命令することが出来る。同様に、付属データ処理装置は、表示メッセージ・ファイル30からVFIT返答メッセージ18に表示データを入れることが出来る。更に暗号アルゴリズム28がVFIT返答メッセージ28の一部分31を暗号化する。随意選択による表示データがない場合、この結果FIT項目19の一部分が2重に暗号化されることがある。FIT表10に貯蔵されているPINキーが、マスター・キーを使つて既に暗号化されているから、この結果2種類の異なるキーを使つて、FIT項目19が3重に暗号化される可能性がある。

口座ファイルに一括処理する為に、自分自身の顧客に対する取引データを顧客データ・ファイル29にアセンブルするだけでよい。この後、取引要請メッセージを端末装置1からサブホスト11が受取つた時、この要請を処理する為に必要な全てのデータは、初めからあるにしても、或いはホスト27から求めたものにしても、そのファイル29から利用し得る。

この発明の別の実施例として、端末FIT8は、端末装置1を所有するか又はその他の形で管理する銀行の種々の書式だけに対する項目と、主体FIT10が管理する協働する銀行に対する全てのFIT項目とを貯蔵し、こうして銀行員又はその他によるFIT8の呼出しにつき、システムの保安性を高めることが出来る。所定の銀行に対するFIT項目は、1回の取引を実行する間、端末装置1に保存してあればよく、その後追放する。

この発明の更に別の実施例として、銀行がその発行カードの基本を成る書式から別の書式に変えることが出来る。この変更の際、同一の機関ID

付属データ処理装置11は主体データ処理装置27にも接続し得る。これは銀行の中央のホスト、交換所システムの全ての会員に対する中央のホスト、または適当な交換通信リンクを介してサブホスト11から連絡し得る交換所システムの別の会員のホスト又はサブホストであつてよい。

付属データ処理装置11は、VFIT取引要請メッセージ17から得られた機関ID及びトラック状態に対するFIT10内の対応する項目を含めて、VFIT返答メッセージ18を端末装置1に通信する手段になる。取引要請メッセージを発生する端末装置1内でのデータ処理と並列に、サブホスト11は主体データ処理装置17を呼出して、前にVFIT取引要請メッセージで通信したデータ中に確認された個人に対し、端末装置1から取引要請を受取ることを予想して、その顧客データ・ファイル29に装入する為に、消費者ファイルを求めることが出来る。この為、付属データ処理装置11は、自分が発行したカードに対する顧客データ・ファイルを管理するか、或いは後で他の

及びトラック状態を持つカードが相異なる2つの書式に関係するのが普通である。符号化トラックにある他のデータを検査する能力のない端末装置1は、その区別が出来ない。こういう場合、発行銀行は、サブホスト11にそのFIT項目だけを管理し、端末装置1が、その発行者に対して顧客から要請された全ての取引を処理する為に、VFIT取引要請メッセージを通じて連絡することを要求する様にすることが出来る。サブホスト11では、適用業務プログラムを設けて、カードの書式を同定するフィールドから読取つたデータの全ての部分或いは他の或る部分を検査し、こうしてサブホスト11が、取引が完了した時、端末装置1の貯蔵装置からそれを追放せよと言う指令と共に、適切なFIT項目を端末装置1に供給出来る様にする。

従つて、以上の説明から判る様に、端末装置1は、それ自体が別の遠隔ホスト27に接続されたサブホストであつてもよいホスト11に接続することが出来、こうしてデータの保安をはかれるよ

うにすると共に、ＦＩＴ表８、１０及びファイル２９の様な顧客口座ファイルを多数の場所に分配することにより、処理及び貯蔵の効率をはかることが出来る。端末装置１に対してＶＦＩＴ返答メッセージ１８で返答しながら、ホスト２７からの口座データをデータ・ファイル２９に入れることにより、ホスト１１は、端末装置１から予想される取引要請に対して、一層敏速に応答することが出来る。

ホスト１１は例えばＩＢＭ３６０１制御装置又はＩＢＭシステム３７０データ処理装置であつてよい。ホスト２７はＩＢＭシステム３７０であつてよい。ホスト１１は、遠隔ホスト２７に接続される時はサブホストと呼び、その他の時はホストと呼ぶ。いずれの場合も、ホスト及びサブホストと言う言葉は、端末装置１のインターフエイスとして使われる時、互換性を以つて使われる。

次に、第６図について、ＰＩＮ表の項目を説明する。ＰＩＮ表の項目には基本的に３種類ある。Ｔ－２（Ｔ－２のみ又はＴ－２独立）、Ｔ－３（

Ｔ－３のみ又はＴ－３独立）及びＴ－２／Ｔ－３組合せである。項目は表の中で任意の順序で現われ得る。違う種類の項目は同じ発行者ＩＤを持つが、Ｔ－２及びＴ－３独立は組合せＴ－２／Ｔ－３とは相互に排他的である。これらの項目の種類の他に、共通ＰＩＮ表項目を特定することが出来る。共通項目は、特定する場合、ＰＩＮ表の最後にあり、ＰＩＮ表の項目の合うものが見つからなかつたクレジット・カードに対して使われる。ＰＩＮ表の項目は、発行者ＩＤの場所以外、消費者ＩＤの検証に必要な全ての情報を含む。発行者ＩＤの場所は任意の取引の前にホスト１１によつて端末装置１に供給される設定イメージから得られる。裏づけのある各々のカードの種類（Ｔ－２、Ｔ－３、Ｔ－２／Ｔ－３）に対して、ＦＩＴ表８、１０に別の小項目が必要である。次に共通部分４０のフイールド４１－４９を説明する。

共通部分

項目４１の長さ

このバイトを含むＰＩＮ項目の全部の長さ

フラグ４２

ビット０＝１　トラック２だけが支援されている。

ビット１＝１　トラック３だけが支援されている。

ビット２＝１　トラック２独立が支援されている。

ビット３＝１　トラック３独立が支援されている。

ビット４＝１　Ｔ－２／Ｔ－３が支援されている。

ビット５＝０　Ⅱがトラック２上にある。

＝１　Ⅱがトラック３上にある。

ビット４＝１の時だけ使う。

ビット６＝０　１つの不良トラックを持つＴ－２／Ｔ－３カードを処

理する。

ビット６＝１　１つの不良トラックを持つカードを排除する。ビット４＝１の時だけ使う。

発行者ＰＩＮの長さ４３

発行者が受理する最大のＰＩＮの長さ。許容し得る最小値は４である。

ＰＩＮ検査の長さ４４

端末装置によつて有効と認定されるＰＩＮのデイジット数。ゼロであれば、ＰＩＮの検証は行なわない。

発行者ＰＩＮパッド／検査パッドのデイジット４５

ビット０－３は、消費者が送込んだＰＩＮが１６デイジットより少ない場合、端末装置で使われる埋合せデイジット。ＤＥＳ暗号化の為、消費者が送込んだＰＩＮの右に埋合せをして１６デイジットにする。ビット４－７は、発行者が供給したＰＩＮ検査データが１６デイジットより少ない場合に使う埋合せデイジットであり、カードから

のＰＩＮ検査データの右側に埋合せ、ＤＥＳ暗号化用の１６デイジットにする。

ＰＩＮキー４６

ＰＩＮの暗号化並びにＰＩＮの有効認定の為に使われる、発行者が供給したキー。ＰＩＮキーはマスター・キーで暗号化される。

１０進変換表４７

ＰＩＮの有効認定に使われる発行者から供給される表。クレジット・カードのＰＩＮ検査データの暗号化により、１６個の１６進デイジットが発生されるが、これを１０進デイジットに変換しなければならない。各々の１６進デイジットは１０進デイジットに置換えられるが、この表（０－１５）内でのその位置が、取替えようとする１６進デイジットの値（０－Ｆ）に対応する。変換が行なわれたら、必要な場合、変換結果にずらし値を加え、次に計算したＰＩＮと消費者のＰＩＮとの比較を行なう。

発行者ＩＤの長さ４８

ＩＤフィールドのバイト数で表わした長さ。

発行者ＩＤ４９

これは、ＰＩＮ表の項目の選択に使われる発行者ＩＤを含む。発行者ＩＤフィールド全体がX′ＦＦ′であることは、共通ＰＩＮ表現項目を表わす。これはＰＩＮ表の最後の項目でなければならない。

次に、Ｔ－２のみ部分のフィールド５１－５４とＴ－２独立フィールド５０を説明する。

ＰＩＮずらし及びＰＩＮ検査の位置５１

ビット０－３は、ＰＩＮずらしＴ－２に対するフィールド分離子の数。ビット４－７は、ＰＩＮ検査データＴ－２に対するフィールド分離子の数。

発行者ＰＩＮずらし変位５２

ＰＩＮ項目のフィールド１０に特定された、フィールド分離子の値からトラック上のＰＩＮずらしまでの変位。このフィールドがX′ＦＦ′であれば、ずらしは用いない。

発行者ＰＩＮ検査データの変位５３

ＰＩＮ項目のフィールド５１に特定された、フィールド分離子の値からカード上のＰＩＮ検査データまでの変位。顧客が送込んだＰＩＮとの相関の基準として使う。

発行者ＰＩＮ検査データの長さ５４

カードに記されたＰＩＮ検査データの長さ。１６デイジットより短い場合、端末装置によつて右側に埋合せデイジットを加え、ＤＥＳ暗号化用の８バイトのフィールドにする。

次にＴ－３のみ部分のフィールド９１－９７及びＴ－３独立フィールド９０を説明する。

ＰＩＮずらし及びＰＩＮ検査の位置９１

ビット０－３はＰＩＮずらし、Ｔ－３までのフィールド分離子の数。ビット４－７はＰＩＮ検査データ、Ｔ－３までのフィールド分離子の数。

発行者ＰＩＮずらしの変位９２

ＰＩＮ項目のフィールド９１に特定された、フィールド分離子の値からトラック上のＰＩＮずらしまでの変位。このフィールドがX′ＦＦ′であれば、ずらしは用いない。

発行者ＰＩＮ検査データの変位９３

ＰＩＮ項目のフィールド９１に特定された、フィールド分離子の値からカード上のＰＩＮ検査データまでの変位。顧客が送込んだＰＩＮとの相関の基準に使う。

発行者ＰＩＮ検査データの長さ９４

カードに記されたＰＩＮ検査データの長さ。１６デイジットより短い場合、端末装置によつて右側に埋合せデイジットを加え、ＤＥＳ暗号化用の８バイトのフィールドにする。

Ｔ－３ＰＩＮ再試行の位置９５

ビット０－３はあけてある。ビット４－７はＴ－３ＰＩＮ再試行カウントを含むカード上のフィールドまでのフィールド分離子の数。

Ｔ－３ＰＩＮ再試行の変位９６

カード上のフィールド内のＴ－３再試行カ

ウントの変位。

T－3データ・マップ97

T－3内のどのフイールドを取引要請メッセージで送るかを示す。

次にT－2／T－3部分100のフイールド101－107を説明する。

PINずらし及びPIN検査の位置101

ビット0－3は、フイールド102に特定されたトラック上のPINずらしまでのフイールド分離子の数。ビット4－7は、フイールド103に特定されたトラック上のPIN検査データまでのフイールド分離子の数。

発行者PINずらしの変位102

ビット0はPINずらしトラックの位置。ビット1－7はPIN項目のフイールド101に特定されたフイールド分離子の値から、トラック上のPINずらしまでの変位。このフイールドがX′FF′であれば、ずらしは用いない。

発行者PIN検査データの変位103

ビット0はPIN検査データのトラックの位置。ビット1－7は、PIN項目のフイールド101に特定されたフイールド分離子の値から、カード上のPIN検査データまでの変位。消費者が送込んだPINとの相関の基準に使う。

発行者PIN検査データの長さ104

カードに記されたPIN検査データの長さ。16デイジットより短い場合、端末装置によつて右側に埋合せデイジットが加えられ、DES暗号化用の8バイトのフイールドにする。

T－3PIN再試行105

T－3PIN再試行カウントを持つカード上のフイールドまでのフイールド分離子の数。

T－3PIN再試行の変位106

カード上のフイールド内のT－3再試行の変位。このフイールドがX′FF′であれ

ば、消費者の随意選択によつて再試行カウントが使われる。

T－3データ・マップ107

T－3内のどのフイールドを取引要請メッセージで送るかを示す。

第7A図及び第7B図には、この発明の取引実行装置を実施する最適の様式による動作が例示されている。顧客IDカードを110で読取り、トラック状態並びに発行者の識別符号に応じて、対応するFIT項目について、局地FIT表の探索が111で行なわれる。FIT項目が112でみつかると、取引データがカードから並びにキーボードで送込まれたものから113の所で収集され、ホストに通信（114）する為の取引要請メッセージを作成する。ホストでは、顧客口座ファイルを検査し、取引の以後の実行に関する命令を含む取引返答メッセージが115の所で端末装置に送返される。端末装置は命令を実行し、顧客口座ファイルを適切に更新することが出来る様に、どういう処置をとつたかをホストに知らせる状態メッセージ116をホストに送返す。

顧客IDカードのデータに対応するFIT項目が局地FITの探索で見つからなかつた場合、端末装置が、ホストに対するVFIT取引要請メッセージに必要なデータを117の所で収集する。このVPINデータ収集手順は第9図のフローチャートに示されている。この第9図は、VPINを選択したホストから前に提供された制御128に応答するT－2及びT－3データの選択130－133を示す。

端末装置がホストに対してVFIT取引要請を118の所で連絡し、ホストはそのファイルから暗号化されたVFIT項目を持つ取引返答119をアセンブルする。端末装置が120の所でVFIT項目を有効と認定し、VFIT項目が要請したものに合うか、或いはその他の形で受理されたというVFIT状態メッセージを121の所でホストに連絡する。カードを保有し並びに／又は取引を停止する様にVFIT取引返答メッセージで命令されない場合、端末装置は取引データの収集

に進み、要請を実行する。ＶＦＩＴ取引返答メッセージでそうする様に命令された場合、取引の実行が完了した時、端末装置はホストから受取つたＶＦＩＴ項目を、その局地ＦＩＴ表から１２２、１２３の所で追放する。

この発明の取引実行端末装置並びに取引実行装置は、金融機関の顧客に対して、セルフサービスの能力を持たせる。この端末装置を使うことにより、銀行員の助けを借りずに、然も一日２４時間、多くの銀行機能の取引が出来る。識別データを符号化した磁気ストライプ・カードが金融機関によつて顧客に対して発行され、顧客はこれを使つて、端末装置で取引を開始する。顧客の身元は個人識別番号（ＰＩＮ）によつて検証される。顧客はこの番号を端末装置のキーボードから送込む。

識別データを含む慎重な扱いを要するデータは、その保安を保つ為に暗号化される。暗号化並びにその後の復号は、暗号アルゴリズム及び金融機関の秘密暗号キーを用いて行なわれる。装置の暗号アルゴリズムは、前に述べたThe National

(55)

Bureau of Standards のData Encryption Standards（ＤＥＳ）として提案されたアルゴリズムに選ぶことが出来る。

端末装置は交換所形式で使うことが出来る。即ち、参加した多数のカード発行機関からのカードの所有者が同じ端末装置を使う様にすることが出来る。

顧客の取引を処理する際に使われるデータの表を端末装置に管理しておき、多くの協働するカード発行機関に対する項目を、顧客のカードから読取る機関識別子によつて呼出す。その表の探索によつて合う項目が見つからない場合、ホストに対して要請メッセージを送り、ホストに管理しているマスター表から合う項目を要請する。マスター表の項目を端末装置で使つた後、それを追放することが出来る。こうして、システムの安全性を高めることが出来る。ホスト（又はサブホスト）の消費者ファイルは、端末装置からの取引要請を扱う為にホスト（又はサブホスト）に消費者ファイルを入れることが出来る。

(56)

4.図面の簡単な説明

第１図はこの発明の取引実行装置を表わす機能ブロック図、第２図は第１図に示した取引実行装置に使われる取引端末装置の機能ブロック図、第３図は利用者によつて開始された取引要請が最初は取引端末装置によつて処理される様子を示す動作ブロック図、第４図は第１図に示した取引実行装置に使われる付属／遠隔主体データ処理装置の機能ブロック図、第５図は取引実行装置の機能ブロック図で、典型的な取引の進行中に、取引端末装置とホスト又はサブホスト・データ処理装置とで交される通信メッセージを示す。第６図はホスト／サブホスト・データ処理装置及び取引端末装置に貯蔵される金融機関表の機能ブロック図、第７Ａ図及び第７Ｂ図はこの発明に従つて取引端末装置によつて行なわれる工程を示す動作フローチャート、第８図は第７図のＦＩＴ探索工程の動作フローチャートで、第４図のサブホストの金融機関表を探索する際に行なわれる工程をも示す。第９図は第７図のＶＰＩＮデータ収集工程の動作フ

(57)

ローチャートである。

２・・・カード読取機、５・・・暗号化装置、８・・・金融機関表、１１・・・ホスト、７８・・・通信装置。

出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション
復代理人　弁理士　頓　宮　孝　一

(58)

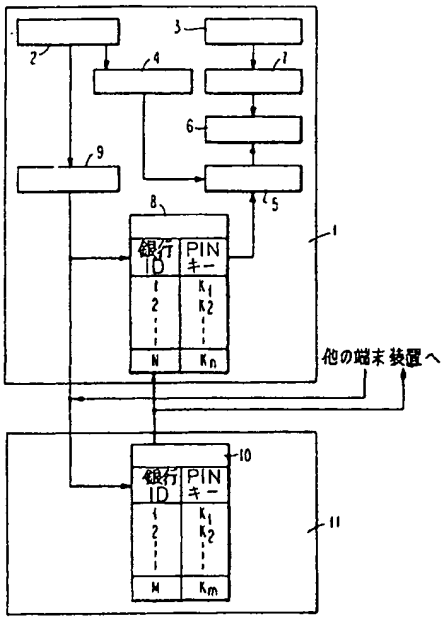
銀行ID
PIN
他の端末装置へ

FIG. 1

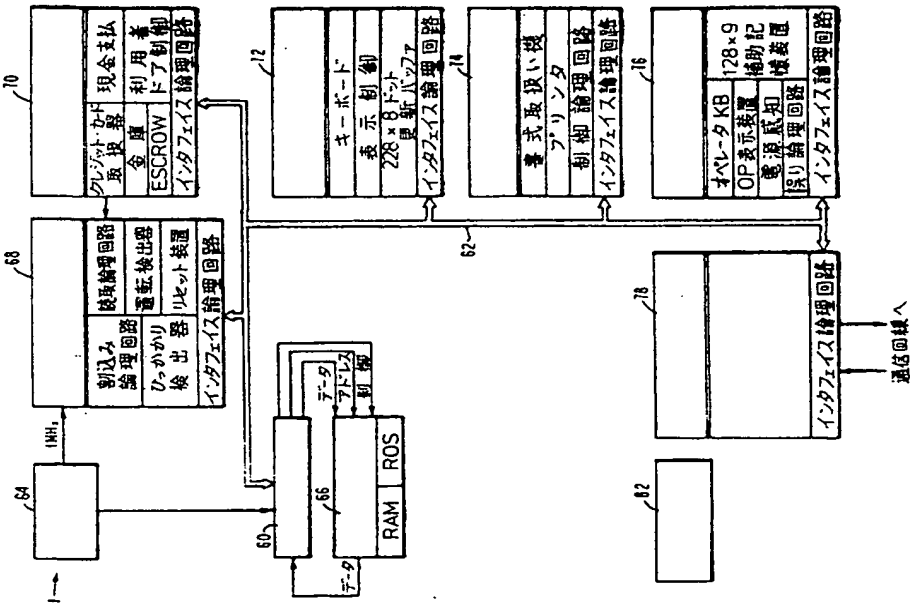
現金支払
利用者ドア制御
インタフェース論理回路
キーボード
表示制御
インタフェース論理回路
プリンタ
制御論理回路
インタフェース論理回路
128×9
インタフェース論理回路
RAM
ROS

FIG. 2

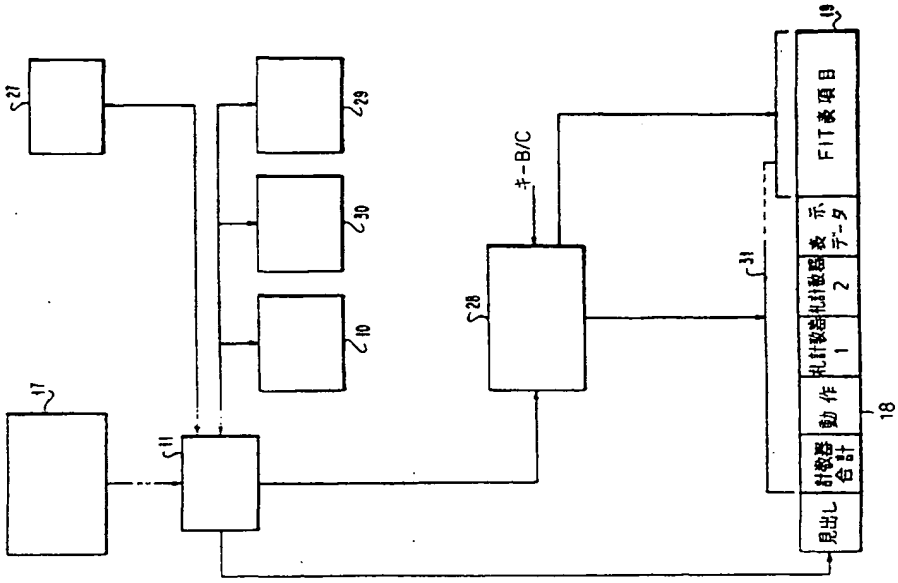
FIT表項目
表示データ
計数器1
計数器2
動作
計数器合計
見出し
キーB/C

FIG. 4

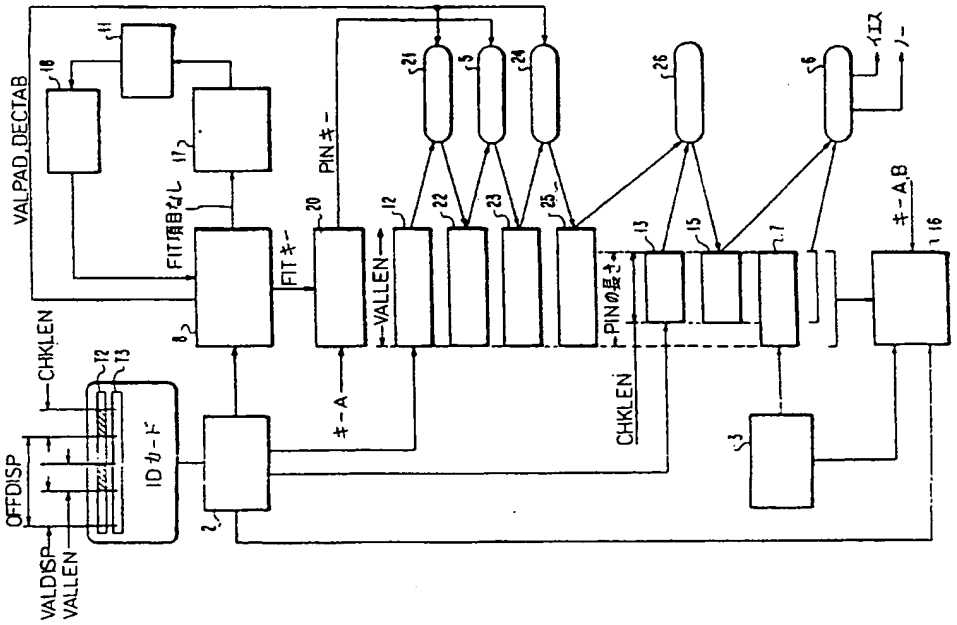
VALPAD_DECTAB
FIT項目なし
FITキー
PINキー
VALLEN
PINの長さ
CHKLEN
キーA
キーA,B
IDカード
OFFDISP
VALDSP
VALLEN

FIG. 3

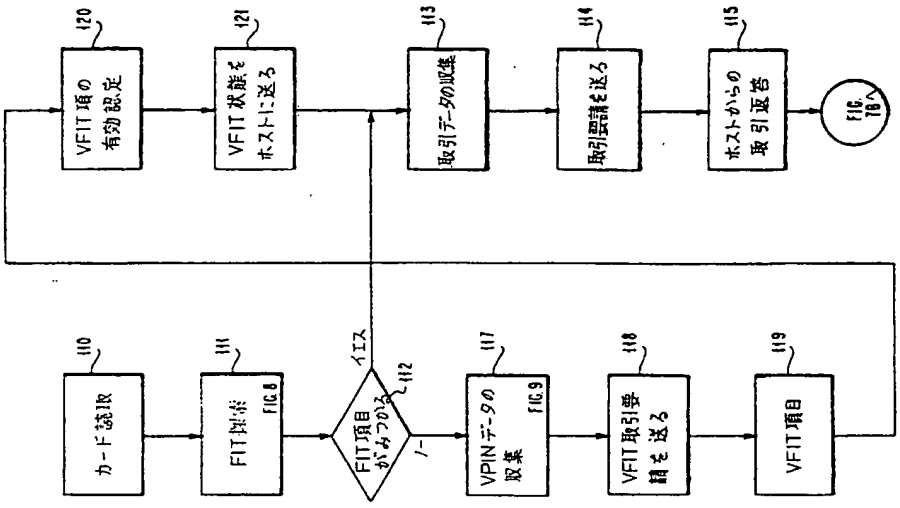

FIG. 7A

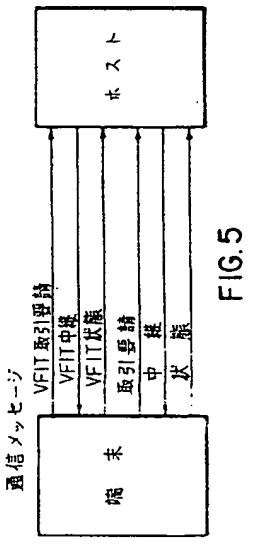

FIG.5

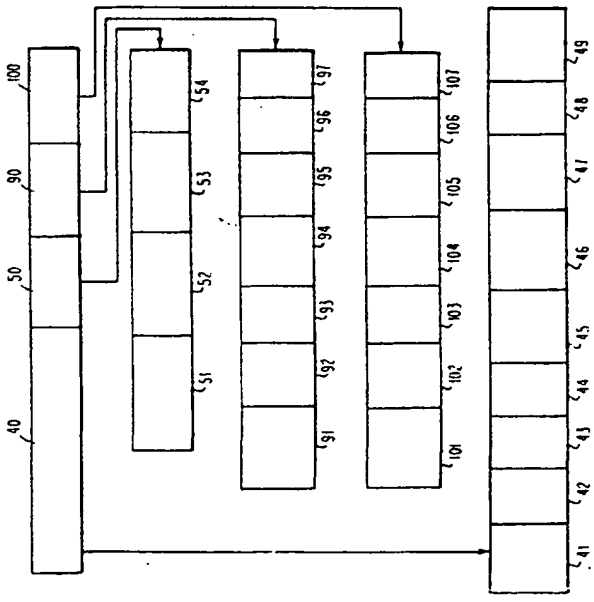

FIG.6

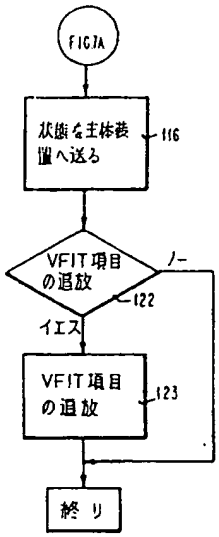

FIG.7B

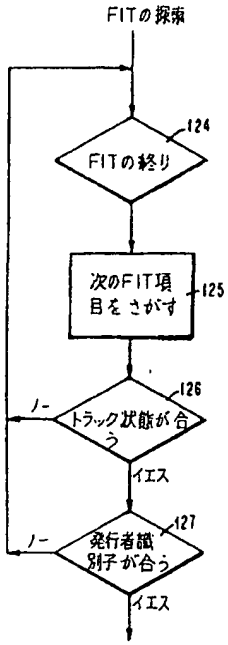

FIG.8

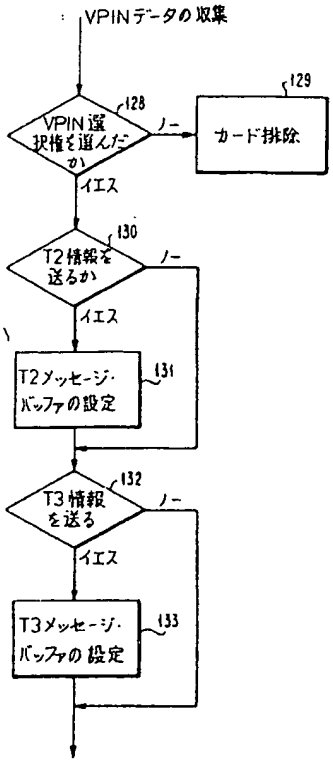

FIG. 9